City of Round Rock

Identity Theft Prevention Program

Management Statement

The City of Round Rock developed and adopted this Identity Theft Prevention Program with all the listed components pursuant to the Federal Trade Commission's (Red Flag) Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The implementation of the program requirements and components will mandate the Identity Theft controls within the City of Round Rock, therefore enhancing the overall security practices and reducing the likelihood of unauthorized individuals gaining access to customer's sensitive information.

James R. Nuse, P.E. City Manager	Hassan Farhat Risk Manager/ Program Administrator

October 2008

Statutory Requirement:
Federal Trade Commission (FTC) – Identity Theft "Red Flags"

The Federal Trade Commission and other regulatory agencies have published the rules and guidelines for regulating the fraudulent attempts to use private and personal information without authority. The new regulations implemented Section 114 (Red Flag Guidelines) and Section 315 (Reconciling address Discrepancies) of the Fair and Accurate Credit Transaction Act (FACTA).

Adoption and Implementation:

The final rulemaking was released by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, The Federal Trade Commission, The National Credit Union Administration, the Office of the Comptroller of Currency, and the Office of Thrift Supervision. The final rules became effective on January 1, 2008; covered financial institutions and creditors must comply with the rules by November 1, 2008. ***The published rules apply to utilities as "creditors" which call for financial institutions and creditors to adopt written Identity Theft Program "Red Flags" by November1, 2008.***

Rule Objective:

The objective of the Identity Theft "Red Flags" Rule is to establish, implement, and document a prevention program to achieve a common minimum security level that protects customer accounts information. This will be accomplished through continuous information/data and gap analysis, risk assessment, policies and procedures, and Identity Theft Program implementation.

Expected Desirable Results:

- Identity Theft controls will prevent information exposure and help identify attempts of criminal activities and reduces the probability of success;
- The damage to the City's and Department's reputation, image, and level of trust is significant in comparison to the cost of correcting a successful fraudulent activity;
- Local management assurance that proper safeguards are in place and ensuring compliance with the statutory requirements.
- "The big picture" – the continuous prevention and control efforts will reduce ID theft elsewhere and can lead to support other organizations and government agencies with their fight against false identification crimes.

Identity Theft Program Administration and Oversight:

The City's Risk Manager serves as the Identity Theft Prevention Program Administrator. An Identity Theft Program Privacy Committee will be established and members at ***management level*** will be appointed from the Finance Department, Utility Billing Office, and other affected City Departments dealing with various customer accounts information.

Due to the sensitive nature of the Program, the Committee members will be entrusted to ensure privacy and confidentiality at all times.

Employee Training and Updates:

Affected City employees will receive initial formal training as an introduction to the Identity Theft Prevention Program elements and mandated requirements. Shortly after, specific training will be scheduled to provide more instructions and clarification on detection of "Red Flags" including the prompt reporting and recoding mechanisms. Employees will be provided with the necessary instructions on any updates pertaining to the new rules and/or the implementation of the program.
Supervisors are advised to conduct a review of the related Human Resources Policies and Procedures with all employees

Covered Utility Accounts:

According to the new Rule, all the utility's accounts that are individual utility service accounts held by customers of the utility whether residential or commercial are covered by the Rule. Identity theft fraud in relation to utility accounts and/or other City customer's accounts involves obtaining the benefit of service using someone else's ***Identifying Information***.

What is Identity Theft?

According to the Fair and Accurate Transaction Act (FACTA), Identity Theft is defined as a fraud committed using the identifying information of another person. Note that Identity Theft is fraud, not theft.

Two Types of Identity Theft Fraud

1 - Relating to new Customer accounts:
- Establishing utility service or other City service using another person's name identifying information;
- The suspected individual defaulted on a past accounts – unable to receive service using the real name;
- The suspected individual intends to establish fraudulent proof of residency in an attempt to commit a fraudulent act somewhere else.

2 - Relating to existing customer accounts:
- Continuing utility service under another customer's name after moving out;
- The suspected individual attempts to avoid paying for service;
- The suspected individual defaulted on past accounts and avoids using the real name.

What is Identifying Information?

Is defined under the Rule as "any name, or number that may be used, alone or in conjunction with any other information, to identify a specific person" including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or tax payer identification number, electronic identification number, internet address, or a routing code.

What is a "Red Flag"?

"Red Flag" is identified as a pattern, practice, or specific activity that indicates the possible existence of identity theft. Examples provided by regulatory agencies: Personal identifying information showing inconsistency when compared against other information sources used by the creditor or the financial institution (address, social security numbers, etc.)

Identifying and Detecting "Red Flags":

In addition to the Utility Billing services, the City of Round Rock provides other services to citizens and manages a variety of customer accounts. In order to identify the Red Flags associated with the nature of the provided services, Utility Billing and other City services must review their type of accounts, the process and mechanism it provides to open an account, the means and methods to access account information, the City's history with fraud and identity theft. The following **Red Flags** are identified by categories:

- ***Warnings from Credit Reporting Agencies:***

  - ✓ Reports of fraudulent activities;
  - ✓ Credit agency alert on a customer;
  - ✓ Credit freeze pending investigation; and
  - ✓ Unusual pattern of customer activities available to the credit agency.

- ***Suspicious Documents and Provided Information:***

  - ✓ Presented documents appear to be forged or altered;
  - ✓ The photograph ID does not match the customer's physical descriptions;
  - ✓ The customer application for service appears to be altered or forged;
  - ✓ Presented documents or information is not consistent with the existing customer information.

- ***Suspicious Personal Identifying Information:***

  - ✓ Presented customer Identifying Information is inconsistent with other provided documented information;

- ✓ Presented customer Identifying Information is inconsistent with information provided by other sources such as government or credit report;
- ✓ Presented customer Identifying Information is consistent with a suspected fraudulent activity (invalid phone number or physical address);
- ✓ The provided social security number matches another customer;
- ✓ Incomplete application for service in an attempt to avoid providing Identifying Information;
- ✓ Other suspicious document inconsistencies detected during the process of requesting services.

- ***Suspicious Account Activity or Unusual Use of Account;***

  - ✓ Returned mail as undeliverable;
  - ✓ Notice of an unauthorized activity;
  - ✓ Detected unusual or very high or very low activity;
  - ✓ Notice by the customer that he/she is not receiving mail sent by Utility Billing;
  - ✓ Detected unauthorized access to account information;
  - ✓ Utility Billing computer security system breach;
  - ✓ Unusual request by customer to change the name on the account.

- ***Alert from other parties;***

  - ✓ Notice from a Utility Billing Customer;
  - ✓ Notice from Law Enforcement;
  - ✓ Notice from another person;
  - ✓ Reporting that an individual, knowingly and willingly, has opened and is maintaining a fraudulent account for a customer engaged in Identity Theft.

City Employee and Supervisor's Responsibility:

New and existing customer accounts…

- ✓ Verify the validity of their request for any changes;
- ✓ Obtain and verify **All** required customer information;
- ✓ Verify the financial institution account information;
- ✓ Verify customer identity;
- ✓ Review carefully all provided documentation;
- ✓ Contact the customer for clarification;
- ✓ Always report and monitor unusual activities or transactions;
- ✓ Do not underestimate any unusual activity;
- ✓ When in doubt, check it out.

City of Round Rock Policy Statement on Security:

"The City makes all efforts to maintain secure operations to safeguard employees, customers, resources, and assets through ongoing risk assessment, loss prevention strategies, and site security of all facilities while respecting civil rights and fundamental freedom."

Related City Policies:

Human Resources Policies and Procedures Manual
Section 1:04 – Maintaining Applicant Files
Section 1:11 – Personal Records and Privacy
Section 5:02 – Privacy Expectations
Section 5:03 – Ethical Standards
Section 5:14 – Whistle Blower Policy
Section 6:01 – Communication
Section 6:02 – Request for Public Information
Section 6:03 – Internal and External Electronic Communications
Section 7:07 – Reporting Accidents, Incidents, and Unusual Events
Department/Division Physical Security Plan
Department/ Division Security Guidelines
Department/ Division Policies and Practices

Customer's Information and Records Protection:

For Employees and Supervisors:

In order to protect the customer *Identifying Information* and to prevent the likelihood of Identity Theft occurring to your customer's accounts (Utility Billing and others), the involved City employees must take several important and critical steps:

- Ensure that all employees are trained on the Identity Theft Prevention Program (Red Flags) and on the related City's Policies and Procedures;
- Ensure that all employees follow the physical security access procedures and that the electronic workstations and websites are properly secured at all times (computer screens, passwords, etc.);
- Ensure that all offices are kept clear of paper with sensitive and identifying information. Secure documents properly or complete destruction of paper documents and computer records containing customer's information;
- Keep only customer information and records that are required and necessary for the business transaction at your worksite.

Incident (Red Flag) Reporting and Fraud Investigation:

If the employee suspects or detects any unusual activities involving potential fraud, the employee must report it immediately to the direct supervisor or the Division supervisor. The supervisor informs the Program Administrator immediately for further inquiry and prompt intervention as appropriate. An initial written record of the activity must be completed by the reporting employee and his/her supervisor.

The following measures are recommended to prevent and mitigate the situation based on level of risk involved and the available information:

- Review and continue to monitor the customer account information;
- Consult with your supervisor and the Program Administrator before contacting the affected customer;
- The Program Administrator will contact the Round Rock Police Department after establishing adequate information for prompt response;
- Avoid opening a new customer account, close the existing account, or reopen the account with a new number.
- Record the event and continue to monitor if necessary.

Program Review and Revision:

The Rule requires that the Identity Theft Prevention Program to be reviewed and evaluated periodically to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft. The City of Round Rock will review the program after three months of implementation and then once every six months to ensure effectiveness, accuracy, and consistency.

The Identity Theft Prevention Program Administrator and Privacy Committee members **(NAMES)** provide guidance and conducts the formal review and update of the program. A review and revision report will be generated and submitted to the City's management staff.

Program Recordkeeping System:

- Rules Updates
- Identity Theft Prevention Program
- Employee Training Records
- Program Review and Revision Periodic Report
- Incident "Red Flag" Reports
- Internal Investigation Reports and Case Associated Records
- Police Reports
- Other Related Records

Affected Departments and Divisions will appoint a designee/an office manager (A name and a job title is required) to ensure that all related program records are kept at a

centralized location and maintained as appropriate. The Identity Theft Prevention Program Administrator will conduct audits at all identified recordkeeping locations to ensure compliance.

Compliance and Practices:

Creditors or financial organizations that do not comply with the requirements risk the threats of fines and/or civil litigations. Creditors are subject to future audits and investigations for various reasons. Once an investigation has been conducted and proof of non-compliance was detected, fines and civil litigations usually will follow from a number of regulatory agencies organizations:

Federal Trade Commission (FTC) – Is authorized to bring enforcement actions in federal court of violations. In some cases, the FTC may bring an action for up to $2,500 in penalties for each independent violation of the rule.

State Enforcement – The states are also authorized to bring actions on behalf of their residents and may recover up to $1,000 for each violation. The States may recover its attorney's fees if successful in each action.

Civil Liability – Individual consumers may be entitled to recover actual damages sustained from a violation. This could be very large and consumers may be able to bring a class action suit seeking potentially massive damages. In addition, successful plaintiffs may recover reasonable attorney's fees.

Disciplinary Action:

All City employees are required to adhere to the City's Human Resources Policies and Procedures and adopted policies and practices. City employees violating the City policies, documented practices, and the applicable statutory rules and regulations are subject to disciplinary actions including termination of employment.

City Employee Personal Identity Theft Awareness:

Consistent with the City policies and procedures on managing records and on protecting sensitive employee information and the privacy and confidentiality practices, it is very critical that all Departments and Divisions dealing with employee personal information to adhere to the noted policies. It is advised that supervisors and employees to have a secure and protected recordkeeping system (electronic or paper); properly discard any unnecessary employee personal information; and to consult with the Human Resources Department on any matters pertaining to employee personal information before it is released.

The City provides periodic Identity Theft Prevention training to all employees in an effort to help protect their personal information. Attached are documents of recommended steps by the Texas Government, Office of the Attorney General advising to be followed if we were victims of identity theft activity. Consult with the Human Resources Department to provide you with other available resources for employee assistance:

Attached: Department/ Division Security Guidelines.